Fuga de información de MERNIS

Visión del analista

El 3 de abril de 2016 se hacía pública la filtración de una base de datos asociada al Sistema Central de Gestión de la Población (MERNIS, por sus siglas en turco) dependiente del Ministerio de Interior Turquía que contenía 49 611 709 registros relativos a ciudadanos turcos. Entre la información filtrada se han identificado campos que muestran el documento de identificación, nombre y apellidos en caracteres ASCII del ciudadano, nombre de pila de los progenitores, ciudad y fecha de nacimiento, sexo y dirección postal completa (incluyendo ciudad, distrito, calle y puerta). Los motivos de la filtración parecen ser *hacktivistas* ya que la persona que publica la información hace referencia a la situación política y religiosa de Turquía, que califica de extremista.

Aunque los registros no incluyen credenciales de acceso, la exposición de información personal puede ser utilizada en prácticas de suplantación de ciudadanos turcos o incluso para la falsificación documental al ofrecer detalles concretos sobre números de identificación personales y lugares de residencia, siendo potencialmente sensibles los detalles de perfiles reconocidos. Asimismo, el nivel de concreción de estos registros ofrece información de utilidad en procesos de desambiguación de ciberidentidades en el marco de investigaciones que tienen lugar en la red y que también podrían ser utilizados fraudulentamente en prácticas de extorsión.

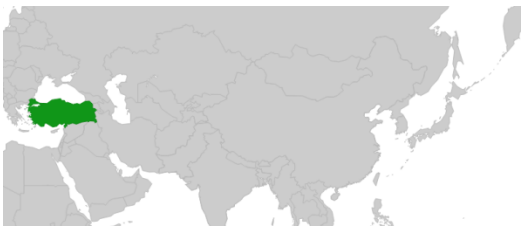
Ficha técnica

Objetivo del ataque:	**MERNIS**
Sector:	**Gubernamental**
Fecha del ataque:	**03/04/2016**
Motivación:	**Hacktivismo**
Autoría:	**Desconocida**
Activos afectados:	**Base de datos de usuarios PostgreSQL**
Naturaleza de la información filtrada:	**Información personal**
Volumen de información:	**49 611 709 registros (confirmado)**
Disponibilidad en línea:	**SÍ**

T.C. İÇİŞLERİ BAKANLIĞI
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü

Presencia del organismo:

Local



Detalles de la filtración

A fecha de publicación de este informe, el archivo comprimido `mernis.tar.gz` se encuentra disponible en al menos un Torrent y una Magnet URL, con más de 1,5 GB de información comprimidos. El archivo contiene dos únicos ficheros: `data_dump.sql` y `data_dump.sql.sha512`. El primero de ellos almacena el volcado completo de la base de datos alcanzando 7 077 350 034 B (6,6 GB), mientras que el segundo contiene el sha512 del primer fichero.

Entre la información disponible, se encuentra el esquema de la tabla de usuarios de una base de datos PostgreSQL, que solamente contiene una tabla `citizen` cuyos campos son únicamente caracteres ASCII en mayúsculas.

```
CREATE TABLE citizen (
    uid bigint NOT NULL,
    national_identifier text NOT NULL,
    first text NOT NULL,
    last text NOT NULL,
    mother_first text NOT NULL,
    father_first text NOT NULL,
    gender character varying(1) NOT NULL,
    birth_city text NOT NULL,
    date_of_birth text NOT NULL,
    id_registration_city text NOT NULL,
    id_registration_district text NOT NULL,
    address_city text NOT NULL,
    address_district text NOT NULL,
    address_neighborhood text NOT NULL,
    street_address text NOT NULL,
    door_or_entrance_number text NOT NULL,
    misc text NOT NULL

);
```

La primera constancia de los enlaces se tiene desde la dirección IP `185.100.87.XX` situada en Bucarest, Rumanía, siendo su ISP FlokiNET ehf.

La filtración se encuentra disponible desde el 3 de abril. El servidor desplegado parece no mostrar modificaciones desde entonces y presenta el mismo ETag a fecha de redacción de este documento que la que identificaba Shodan a 4 de abril.

El autor en su reivindicación hace mención explícita al Presidente de Turquía Recep Tayyip Erdogan, de quien afirma literalmente que «está destruyendo vuestro país», utilizando la segunda persona del plural. Asimismo, y aunque no guarda relación aparente, al final del comunicado, el autor cita al candidato republicano Donald Trump sobre quien lanza una advertencia a los ciudadanos de EEUU.

Posibles usos y recomendaciones generales

La información personal suministrada no expone en sí misma activos tecnológicos concretos. Sin embargo, malas prácticas de seguridad en la elección de contraseñas y preguntas de recuperación sí pueden motivar la explotación de información como el lugar de nacimiento, la fecha o incluso los nombres de los familiares. En el caso de personalidades de la vida política y social, esta información expondría lugares de residencia que no tienen por qué ser de dominio público.

La información identificada se componía de un volcado masivo de la base de datos facilitada en forma de fichero de texto `.sql` para ser cargado en una base de datos. Por este motivo, la criticidad de la fuga se verá incrementada en el momento en que aparezcan servicios de consulta de la información en la red de forma estructurada empleando interfaces de búsqueda al uso, lo que no se descarta dada la facilidad que entrañaría el procesamiento de cada registro al estar delimitados sus campos.